ABSTRACT

Method and Apparatus for Discovering a Trust Chain Imparting a Required Attribute to a Subject

A method is disclosed for discovering a trust chain that imparts a required attribute to a subject and is grounded in a trusted principal that is the issuer of a known trusted attribute delegation. The method involves setting as a primary goal to be proved an attribute delegation from a trusted principal to the subject and then seeking a backwards proof of the primary goal by a process of recursively taking a goal to be proved, starting with the primary goal, and decomposing it into subgoals one of which corresponds to an attribute delegation already proved by an available certificate. If it is not possible to decompose a subgoal that has not been proved, the process backtracks to a previous subgoal to seek a new decomposition of the latter. A trust chain is taken as found when the process produces a chain of subgoals proved by corresponding certificates, that grounds in a subgoal proved by a trusted attribute delegation. Name mappings are also permitted.

(Fig. 9)